

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-052029

(43)Date of publication of application : 21.02.2003

(51)Int.Cl.

H04N 7/16

G06F 17/60

H04L 9/08

(21)Application number : 2001-237326

(71)Applicant : NEC CORP

(22)Date of filing : 06.08.2001

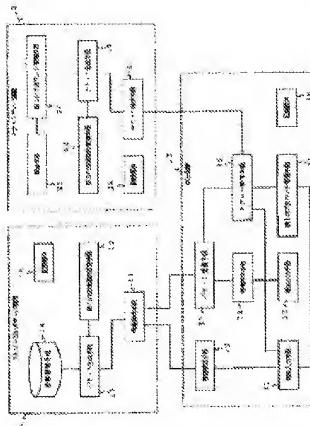
(72)Inventor : NAKAE MASAYUKI

(54) INFORMATION PROVIDING DEVICE, TICKET PROVIDING DEVICE, REPRODUCING DEVICE AND INFORMATION SELLING METHOD AND ITS PROGRAM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide an information selling system for allowing the sales person of information to freely set the selling condition of information owned by the sales person himself or herself, in an information selling configuration that the sales person of information is different from the operator of a streaming system.

SOLUTION: This streaming system is provided with a streaming server device 1 to be managed by the operator of this system, a ticket server device 2 to be managed by the sales person of information, and a reproducing device 3 to be used by a user. The streaming server device 1 and the ticket server device 2 are respectively provided with a first transmission terms of agreement managing means 12, and a second transmission convention managing means 22 for individually managing a transmission terms of agreement prepared based on the consignment contract of the information distribution processing preliminarily concluded between the sales person of the information and the operator of the streaming system.



(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2003-52029

(P2003-52029A)

(43)公開日 平成15年2月21日(2003.2.21)

(51)Int.Cl. ⁷	識別記号	F I	テクニコト*(参考)
H 04 N 7/16		H 04 N 7/16	C 5 C 0 6 4
G 06 F 17/60	3 0 2	G 06 F 17/60	3 0 2 E 5 J 1 0 4
	3 3 2		3 3 2
	5 1 2		5 1 2
	Z E C		Z E C
審査請求 有		請求項の数32	O L (全 31 頁) 最終頁に続く

(21)出願番号 特願2001-237326(P2001-237326)

(71)出願人 000004237

日本電気株式会社

東京都港区芝五丁目7番1号

(22)出願日 平成13年8月6日(2001.8.6)

(72)発明者 中江 政行

東京都港区芝五丁目7番1号 日本電気株
式会社内

(74)代理人 100088812

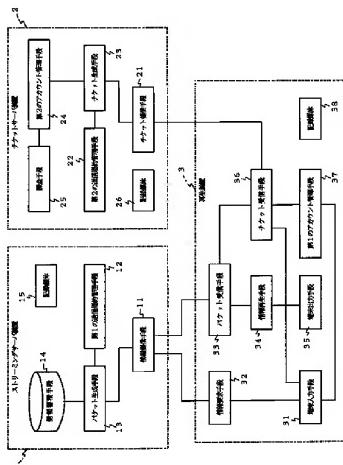
弁理士 ▲柳▼川 信

(54)【発明の名称】 情報提供装置、チケット提供装置、再生装置及びそれに用いる情報販売方法並びにそのプログラム

(57)【要約】

【課題】 情報の販売者とストリーミングシステムの運用者とが異なるような情報販売形態において、情報の販売者が自己の所有する情報の販売条件を自由に設定可能な情報販売システムを提供する。

【解決手段】 ストリーミングシステムの運用者が管理するストリーミングサーバ装置1と、情報の販売者が管理するチケットサーバ装置2と、利用者が使用する再生装置3とを備えるシステムにおいて、予め情報の販売者とストリーミングシステム運用者との間で結ばれた情報配信処理の委託契約に基づいて作成された送信規約を個別に管理するための第1の送信規約管理手段1.2及び第2の送信規約管理手段2.2をそれぞれストリーミングサーバ装置1及びチケットサーバ装置2に備えている。



【特許請求の範囲】

【請求項1】 情報をユーザに提供する情報提供装置であって、前記情報を暗号化するための情報暗号鍵と前記ユーザに対する販売条件とを少なくとも含む第1の送信規約を管理する第1の送信規約管理手段と、前記ユーザからの情報要求時に前記情報暗号鍵を用いて暗号化した情報を単に前記ユーザに送信する情報提供手段とを有することを特徴とする情報提供装置。

【請求項2】 前記ユーザからの情報要求時にその情報要求メッセージを受信する度に当該メッセージの送信元と通信しながら前記情報暗号鍵を変形するための情報を示すセッション鍵を確立するセッション鍵確立手段と、前記情報暗号鍵を当該セッション鍵を用いて変形させた鍵によって前記情報を暗号化する第2のパケット生成手段とを含むことを特徴とする請求項1記載の情報提供装置。

【請求項3】 前記情報は、その受信と再生とが並列的に行われるストリーミングデータであることを特徴とする請求項1または請求項2記載の情報提供装置。

【請求項4】 ユーザに対する情報提供時に前記ユーザに対する認証処理と課金処理とを行うチケット提供装置であって、暗号化された情報を復号して再生可能とするための情報復号鍵と前記ユーザに対する販売条件とを少なくとも含む第2の送信規約を管理する第2の送信規約管理手段を有することを特徴とするチケット提供装置。

【請求項5】 情報をユーザに販売するにあたって予め蓄積された当該ユーザの利用者情報及び当該ユーザの使用装置情報を含むクライアント情報と前記第2の送信規約とを基に当該ユーザの認証処理を行う第2のアカウント管理手段と、前記第2の送信規約を基に前記ユーザに対する課金処理を行う課金手段とを含むことを特徴とする請求項4記載のチケット提供装置。

【請求項6】 前記第2の送信規約の有無と、前記第2の送信規約に記載されかつ少なくとも有効期間を含む有効性に関する条件と、前記ユーザのクライアント情報の正当性とをそれぞれ判定してそれらのいずれかが無効と判定した時に前記ユーザに対して前記情報復号鍵を含むチケットの発行を抑止するチケット生成手段を含むことを特徴とする請求項5記載のチケット提供装置。

【請求項7】 前記第2の送信規約を管理する複数の第2の送信規約管理手段と、前記チケットの要求時にその要求内容に応じて前記複数の第2の送信規約管理手段のうちのいずれかを選択する送信規約グループ管理手段とを含むことを特徴とする請求項6記載のチケット提供装置。

【請求項8】 前記情報は、その受信と再生とが並列的に行われるストリーミングデータであることを特徴とする請求項4から請求項7のいずれか記載のチケット提供装置。

【請求項9】 情報提供装置から提供されかつ情報を暗

号化するための情報暗号鍵を用いて暗号化された情報を、チケット提供装置から提供されかつ前記暗号化された情報を復号して再生可能とするための情報復号鍵を少なくとも含むチケットに基づいて復号しつつ再生可能とするパケット受信手段を有することを特徴とする再生装置。

【請求項10】 前記情報提供装置から前記情報暗号鍵を変形するための情報を示すセッション鍵が送られてきた時にそのセッション鍵を用いて前記セッション鍵で変形された鍵を生成する手段と、その生成された鍵を用いて前記セッション鍵で変形させた鍵によって暗号化された情報を復号する第2のパケット受信手段とを含むことを特徴とする請求項9記載の再生装置。

【請求項11】 前記情報は、その受信と再生とが並列的に行われるストリーミングデータであることを特徴とする請求項9または請求項10記載の再生装置。

【請求項12】 情報を暗号化してユーザに提供するための情報暗号鍵と前記ユーザに対する販売条件とを少なくとも含む第1の送信規約を基に前記情報を暗号化するステップと、その暗号化した情報を前記ユーザからの情報要求時に当該ユーザに送信するステップとを前記情報を提供する情報提供装置に有し、

前記暗号化された情報を復号して再生可能とするための情報復号鍵と前記ユーザに対する販売条件とを少なくとも含む第2の送信規約を基に前記情報の販売時に前記情報復号鍵を含むチケットの発行を行うステップを前記チケットを提供するチケット提供装置に有することを特徴とする情報販売方法。

【請求項13】 前記情報の販売時に予め蓄積された前記ユーザの利用者情報及び当該ユーザの使用装置情報を含むクライアント情報と前記第2の送信規約とを基に当該ユーザの認証処理を行うステップと、前記第2の送信規約を基に前記ユーザに対する課金処理を行うステップと前記チケット提供装置に含み、

要求された情報を前記ユーザに送信するにあたって前記情報提供装置が前記暗号化された情報の送出を単に行うようにしたことを特徴とする請求項12記載の情報販売方法。

【請求項14】 前記第2の送信規約の有無と、前記第2の送信規約に記載されかつ少なくとも有効期間を含む有効性に関する条件と、前記ユーザのクライアント情報の正当性とをそれぞれ判定してそれらのいずれかが無効と判定した時に前記チケット提供装置が前記ユーザに対して前記チケットの発行を抑止するようにしたことを特徴とする請求項13記載の情報販売方法。

【請求項15】 前記チケット提供装置は、前記チケットを要求するメッセージの内容に応じて前記第2の送信規約を管理する複数の第2の送信規約管理手段のうちのいずれかを選択するようにしたことを特徴とする請求項12から請求項14のいずれか記載の情報販売方法。

【請求項16】 前記チケットを要求するメッセージを前記チケット提供装置に送信するステップと、前記メッセージに応答して適切な情報復号鍵を含むチケットを得た時に当該チケットを基に前記情報提供装置で暗号化された情報を復号しつつ再生可能とするステップを前記情報を再生使用する再生装置に含むことを特徴とする請求項12から請求項15のいずれか記載の情報販売方法。

【請求項17】 前記情報を要求するメッセージを受信する度に当該メッセージの送信元である前記再生装置と通信しながら前記情報暗号鍵を変形するための情報を示すセッション鍵を確立するステップと、前記情報暗号鍵を当該セッション鍵を用いて変形させた鍵によって前記情報を暗号化するステップとを前記情報提供装置に含み、

前記情報提供装置から前記セッション鍵が送られてきた時にそのセッション鍵を用いて前記セッション鍵で変形された鍵を生成するステップと、その生成された鍵を用いて前記セッション鍵で変形させた鍵によって暗号化された情報を復号するステップとを前記再生装置に含むことを特徴とする請求項16記載の情報販売方法。

【請求項18】 前記情報提供装置は、販売対象となる情報と当該情報を対応する前記第1の送信規約とを管理し、

前記チケット提供装置は、前記情報に対応する前記第2の送信規約を管理するようにしたことを特徴とする請求項12から請求項17のいずれか記載の情報販売方法。

【請求項19】 前記チケット提供装置は、前記情報の代金をユーザから徴収した時に前記チケットを前記ユーザに提供するとともに、前記情報の代金の徴収時に前記情報提供装置の運用者に対して所定の委託契約に基づいた配信手数料を支払うようにしたことを特徴とする請求項12から請求項18のいずれか記載の情報販売方法。

【請求項20】 前記情報提供装置が前記暗号化された情報の提供を専ら行い、前記チケット提供装置が前記販売条件にしたがった適切な課金及び正当と認められるユーザに対する前記チケットの提供を行うようにしたことを特徴とする請求項12から請求項19のいずれか記載の情報販売方法。

【請求項21】 前記販売条件の変更及び前記情報の販売停止を行う時に、前記チケット提供装置で前記第2の送信規約の変更及び破棄を行うようにしたことを特徴とする請求項12から請求項20のいずれか記載の情報販売方法。

【請求項22】 前記情報の配信に係る委託を複数の情報提供装置の運用者に対して行う時に前記チケット提供装置の運用者と前記情報提供装置の運用者との間で個別に締結された委託契約に基づいて作成される販売条件の組を前記チケット再生装置に登録し、前記販売条件に対応する前記第1の送信規約を前記情報提供装置で管理し、前記販売条件に対応する前記第2の送信規約を前記

チケット提供装置で管理するようにしたことを特徴とする請求項12から請求項21のいずれか記載の情報販売方法。

【請求項23】 前記再生装置の利用者が前記暗号化された情報を提供を受ける際に、前記再生装置から前記チケット提供装置に当該利用者の識別や課金に必要な情報を送信し、前記再生装置が前記チケット提供装置から前記チケットを取得して前記暗号化された情報を復号しながら再生するようにしたことを特徴とする請求項12から請求項22のいずれか記載の情報販売方法。

【請求項24】 前記情報は、その受信と再生と共に並列的に行われるストリーミングデータであることを特徴とする請求項12から請求項23のいずれか記載の情報販売方法。

【請求項25】 コンピュータに、暗号化された情報を復号して再生可能とするための情報復号鍵を少なくとも含むチケットを要求するメッセージを受信する処理と、その受信したメッセージから前記情報を識別するための情報識別子を抽出する処理と、この抽出された情報識別子を基に前記情報復号鍵とユーザに対する販売条件とを少なくとも含む複数の第2の送信規約のうちのいずれかを選択する処理と、前記メッセージの正当性を確認する処理と、選択された第2の送信規約に記載された課金額分の課金を行なう処理と、選択された第2の送信規約に基に前記チケットを生成する処理とを実行させるためのプログラム。

【請求項26】 前記コンピュータに、受信したメッセージから運用者識別子及び前記情報識別子からなる識別子を抽出する処理と、抽出した識別子を前記運用者識別子及び前記情報識別子に分割する処理と、分割された運用者識別子に対する第2の送信規約の集合を選択する処理と、選択した第2の送信規約の集合の中から前記情報識別子に対応する送信規約を選択する処理とをさらに実行させることを特徴とする請求項25記載のプログラム。

【請求項27】 コンピュータに、情報を要求するメッセージを受信する処理と、その受信したメッセージから前記情報を識別するための情報識別子を抽出する処理と、抽出した情報識別子を基に前記情報を暗号化するための情報暗号鍵とユーザに対する販売条件とを少なくとも含む複数の第1の送信規約のいずれかと当該情報を選択する処理と、前記第1の送信規約に記載された情報暗号鍵によって前記情報を読みながら暗号化を行なう処理とを実行させるためのプログラム。

【請求項28】 前記コンピュータに、前記情報暗号鍵を変形するための情報を示すセッション鍵をランダムに生成して送信する処理と、前記情報暗号鍵を前記セッション鍵で変形させた鍵を生成して保持する処理とをさらに実行させることを特徴とする請求項27記載のプログラム。

【請求項29】 前記コンピュータに、前記情報暗号鍵を変形するための情報を示すセッション鍵を要求しかつて予め設定された第1のセッション鍵を含むメッセージを受信した後に当該メッセージから前記第1のセッション鍵を抽出する処理と、第2のセッション鍵をランダムに生成して送信する処理と、前記第1のセッション鍵と前記第2のセッション鍵とを閑数にかけた値を用いて情報復号鍵を変形させた鍵を生成して保持する処理とをさらに実行させることを特徴とする請求項28記載のプログラム。

【請求項30】 コンピュータに、暗号化された情報を復号して再生可能とするための情報復号鍵を少なくとも含むチケットを要求するメッセージを生成して送信する処理と、前記チケットを受信する処理と、受信したチケットから前記情報復号鍵を抽出して保持する処理と、その抽出した情報復号鍵を用いて受信した情報を復号しながら再生する処理とを実行させるためのプログラム。

【請求項31】 前記コンピュータに、前記情報暗号鍵を変形するための情報を示すセッション鍵を受信する処理と、前記情報復号鍵を前記セッション鍵で変形させた鍵を生成して保持する処理とをさらに実行させることを特徴とする請求項30記載のプログラム。

【請求項32】 前記コンピュータに、前記情報暗号鍵を変形するための第1のセッション鍵をランダムに生成して保持する処理と、前記第1のセッション鍵を含むセッション鍵を要求するメッセージを送信する処理と、第2のセッション鍵を受信した後に前記第1のセッション鍵と前記第2のセッション鍵とを閑数にかけた値を用いて前記情報復号鍵を変形させた鍵を生成して保持する処理とをさらに実行させることを特徴とする請求項30記載のプログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は情報提供装置、チケット提供装置、再生装置及びそれに用いる情報販売方法並びにそのプログラムに關し、特に提供する利用者の性質や時刻等を基にした多様な課金制御を行う情報販売システムに関する。

【0002】

【従来の技術】 従来、インターネットを利用したビデオ／音楽等の情報提供方法としては、情報をいくつかの通信パケットに断片化し、各通信パケットを順次送受信しつゝ、情報を再生していくような「ストリーミング方式」が一般に知られている。以下、ストリーミング方式を利用した情報提供システムを「ストリーミングシステム」と呼ぶ。

【0003】 このようなストリーミングシステムを用いて情報を販売する方法は既に知られており、それを利用した情報販売システムの一例として、特開2001-43440号公報に開示されたシステムや、特開2000

-124900号公報に開示されたシステム等がある。これらのシステムはいずれも、ストリーミングシステム内に課金手段を用意している。したがって、ストリーミングシステムは情報提供処理に加えて、課金に係るユーザ認証処理や課金処理等を同一システム内で行うものである。

【0004】 また、一般的な情報販売システムにおいて、情報の送出処理を専ら行う情報提供システムの外に、ユーザ認証処理や課金処理等を専ら行う課金システムを備えるような情報販売システムも知られており、それについての一例が、特開平11-98136号公報や特開平10-124576号公報等に記載されている。

【0005】 特開平11-98136号公報記載の情報販売システムでは、情報提供システム（「データ提供者のサーバ」）の外に、課金システム（「中継サーバ」）が備えられており、課金システムは、一般によく知られた「プロキシ」として動作する。

【0006】 情報販売システムにおいては、ユーザから情報提供システムへ情報提供を要求するにあたり、課金システムを必ず経由する必要があり、さらに課金システム上でユーザ認証処理や課金処理が行われ、その後、情報提供システムから送出された情報が課金システムを経由してユーザへ伝達される。この場合、課金システムはユーザ認証処理や課金処理に加えて、情報提供処理をも併せて行うことになり、この点において、上記のようなストリーミングシステムと同等といえる。

【0007】一方、特開平10-124576号公報記載の情報販売システムでは、「情報提供装置」及び「鍵管理装置」から構成される情報提供システムと、「情報管理装置」から構成される課金システムとを備えている。

【0008】 ユーザから情報提供システムへ情報提供を要求すると、情報提供システムの情報提供装置から暗号化された情報が送出され、加えて鍵管理装置から暗号化情報の復号鍵が送出される。ここで、各ユーザの利用する端末と、情報提供システムを構成する2つの装置とにそれぞれ、「回線接続装置」が備えられており、課金システムはこれら回線接続装置の識別及び回線接続装置間の通信記録を蓄積することができる。

【0009】 したがって、課金システムはユーザ及び情報提供システムとの間で交わされる情報提供処理に関するすべての記録を基に、適切な課金処理を行なうことができる。しかしながら、課金システムはユーザ及び情報提供システム間の通信を遮断することはできないので、支払い能力の有無やユーザの識別情報の正当性等を検査し、必要に応じて情報提供処理を中断する等といったユーザ認証処理を行なうことができない。

【0010】 また、一般に、インターネット上の情報販売システムにおいては、ユーザ及び情報提供システム間の通信内容が、例えばSSL (Secure Socke

t Layer) 等の暗号化通信方式によって暗号化されている場合が多く見られるが、このような場合に、課金システムでは適切な課金処理を行うことができない。

【0011】

【発明が解決しようとする課題】上述した従来のストリーミングシステムでは、そのシステム上に課金サブシステムや利用者管理サブシステムを構築するため、販売者が価格の操作を行いたい場合や独自の利用者データベースを構築したい場合に、ストリーミングシステム運用者に上記のような各種サブシステムの再設定を依頼しなければならない上に、ストリーミングシステム運用者から見れば委託を受けているあらゆる販売者からの上記のような依頼に応えるのは実務上困難である。

【0012】そのため、情報の販売者が自己の所有する情報の販売にあたって、外部のストリーミングシステム運用者に情報提供業務を委託するような場合、販売者自身が価格を自由に操作したり、販売者独自の顧客管理を行なうことが困難であるという問題がある。

【0013】また、ストリーミングシステムの持つ計算機資源及び通信資源は有限であり、かつ同システム上で利用者認証処理や課金処理を行うと各資源が余計に消費されるので、情報の送信処理に必要な各資源が圧迫される。そのため、ストリーミングシステム上で利用者認証処理や課金処理を行う場合、ストリーミングシステムが行なう送信処理のパフォーマンスを低下させるという問題がある。

【0014】さらに、従来のストリーミングシステムのように、ストリーミングシステム内で利用者認証処理や課金処理を行う場合には、利用者から得られる利益を正確に把握できるのがストリーミングシステム運用者のみであり、情報の販売者はストリーミングシステム運用者からの申告を信頼するよりはかない。

【0015】そのため、上記の問題と同様に、情報の販売者とストリーミングシステムの運用者が異なる場合には、情報提供の対価として利用者から得られる利益を、情報の販売者とストリーミングシステムの運用者とで分配する必要があるが、こうした利益分配が公正に行われる保証がないという問題がある。

【0016】そこで、本発明の目的は上記の問題点を解消し、情報の販売者とストリーミングシステムの運用者とが異なるような情報販売形態において、情報の販売者が自己の所有する情報の販売条件(価格や利用者制限)を自由に設定することができる情報販売システム及び情報販売方法並びにそのプログラムを提供することにある。

【0017】また、本発明の他の目的は、ストリーミングシステムが行なう情報の送信処理のパフォーマンスを低下させることなく、利用者認証処理や課金処理を行うことができる情報販売システム及び情報販売方法並びにそのプログラムを提供することにある。

【0018】さらに、本発明の別の目的は、情報の販売者とストリーミングシステムの運用者とが異なるような情報販売形態において、利用者から得られる利益を、情報の販売者とストリーミングシステムの運用者との間で公正に分配することができる情報提供装置、チケット提供装置、再生装置及びそれに用いる情報販売方法並びにそのプログラムを提供することにある。

【0019】

【課題を解決するための手段】本発明による情報提供装置は、情報をユーザに提供する情報提供装置であって、前記情報を暗号化するための情報暗号鍵と前記ユーザに対する販売条件とを少なくとも含む第1の送信規約を管理する第1の送信規約管理手段と、前記ユーザからの情報要求時に前記情報暗号鍵を用いて暗号化した情報を単に前記ユーザに送信する情報提供手段とを備えている。

【0020】本発明によるチケット提供装置は、ユーザに対する情報提供時に前記ユーザに対する認証処理と課金処理とを行うチケット提供装置であって、暗号化された情報を復号して再生可能とするための情報復号鍵と前記ユーザに対する販売条件とを少なくとも含む第2の送信規約を管理する第2の送信規約管理手段を備えている。

【0021】本発明による再生装置は、情報提供装置から提供されかつ情報を暗号化するための情報暗号鍵を用いて暗号化された情報を、チケット提供装置から提供されかつ前記暗号化された情報を復号して再生可能とするための情報復号鍵を少なくとも含むチケットに基づいて復号しつつ再生可能とするバケット受信手段を備えている。

【0022】本発明による情報販売方法は、情報を暗号化してユーザに提供するための情報暗号鍵と前記ユーザに対する販売条件とを少なくとも含む第1の送信規約を基に前記情報を暗号化するステップと、その暗号化した情報を前記ユーザからの情報要求時に当該ユーザに送信するステップとを前記情報を提供する情報提供装置に備え、前記暗号化された情報を復号して再生可能とするための情報復号鍵と前記ユーザに対する販売条件とを少なくとも含む第2の送信規約を基に前記情報の販売時に前記情報復号鍵を含むチケットの発行を行うステップを前記チケットを提供するチケット提供装置に備えている。

【0023】本発明による他の情報販売方法は、前記情報の販売時に予め蓄積された前記ユーザの利用者情報及び当該ユーザの使用装置情報を含むクライアント情報と前記第2の送信規約とを基に当該ユーザの認証処理を行うステップと、前記第2の送信規約を基に前記ユーザに対する課金処理を行うステップとを前記チケット提供装置に備し、要求された情報を前記ユーザに送信するにあたって前記情報提供装置が前記暗号化された情報の送出を単に行なうようにしている。

【0024】本発明による別の情報販売方法は、前記チ

ケットを要求するメッセージを前記チケット提供装置に送信するステップと、前記メッセージに応答して適切な情報復号鍵を含むチケットを得た時にのみ当該チケットを基に前記情報提供装置で暗号化された情報を復号しつつ再生可能とするステップを前記情報を再生使用する再生装置に具備している。

【0025】本発明による情報販売方法のプログラムは、コンピュータに、暗号化された情報を復号して再生可能とするための情報復号鍵を少なくとも含むチケットを要求するメッセージを受信する処理と、その受信したメッセージから前記情報を識別するための情報識別子を抽出する処理と、この抽出された情報識別子を基に前記情報復号鍵とユーザに対する販売条件とを少なくとも含む複数の第2の送信規約のうちのいずれかを選択する処理と、前記メッセージの正当性を確認する処理と、選択された第2の送信規約に記載された課金額分の課金を行う処理と、選択された第2の送信規約を基に前記チケットを生成する処理とを実行させている。

【0026】本発明による他の情報販売方法のプログラムは、コンピュータに、情報を要求するメッセージを受信する処理と、その受信したメッセージから前記情報を識別するための情報識別子を抽出する処理と、抽出した情報識別子を基に前記情報を暗号化するための情報暗号鍵とユーザに対する販売条件とを少なくとも含む複数の第1の送信規約のいずれかと当該情報を選択する処理と、前記第1の送信規約に記載された情報暗号鍵によって前記情報を読みながら暗号化を行う処理とを実行させている。

【0027】本発明による別の情報販売方法のプログラムは、コンピュータに、暗号化された情報を復号して再生可能とするための情報復号鍵を少なくとも含むチケットを要求するメッセージを生成して送信する処理と、前記チケットを受信する処理と、受信したチケットから前記情報復号鍵を抽出して保持する処理と、その抽出した情報復号鍵を用いて受信した情報を復号しながら再生する処理とを実行させている。

【0028】すなわち、本発明の情報販売システムは、ストリーミングシステムの運用者が管理するストリーミングサーバ装置と、情報の販売者が管理するチケットサーバ装置と、利用者が使用的する再生装置とを備え、ストリーミングサーバ装置に第1の送信規約管理手段を備え、チケットサーバ装置に第2の送信規約管理手段を備えることで、予め情報の販売者とストリーミングシステム運用者との間で結ばれた情報配信処理の委託契約に基づいて作成された送信規約を個別に管理するようにしている。

【0029】また、第1の送信規約管理手段で保持される送信規約が情報暗号鍵を含むようにし、ストリーミングサーバ装置が再生装置に情報を提供する際に、バケット生成手段で、その情報を情報暗号鍵で暗号化したセキ

ュアパケットを生成するようしている。

【0030】さらに、当該セキュアパケットを受信した再生装置は、チケット受信手段で予めチケットサーバ装置から、第2の送信規約管理手段で保持される送信規約に記載された情報復号鍵を含むチケットを受信するようにして、さらにパケット受信手段において、当該情報復号鍵によってセキュアパケットを復号するようにしている。

【0031】さらにまた、チケットサーバ装置と再生装置との間で、上記のようなチケット通信を行う際には、再生装置のチケット受信手段及び第1のアカウント管理手段によって、ユーザから情報の販売者に情報の代金を支払うのに必要な決済用情報、もしくは決済用情報を特定するに十分なユーザID(識別情報)等のアカウント情報などをチケット要求メッセージに含めるようにし、チケットサーバ装置の第2のアカウント管理手段で当該アカウント情報の正当性を確認するようしている。

【0032】加えて、チケット要求メッセージに情報識別子を含めるものとし、チケットサーバ装置の第2の送信規約管理手段から当該情報識別子に対応する送信規約を取得するようにし、送信規約に記載された課金額を課金手段に伝達するようしている。

【0033】上記のように、情報の販売者が自己の所有する情報の販売条件を送信規約として管理するためのチケットサーバ装置を備えることによって、情報の販売者がストリーミングシステムの運用者に情報の配信業務を委託する際に、情報の販売者が自己の所有する情報の販売条件を自由に設定することが可能となる。

【0034】また、利用者認証処理や課金処理をストリーミングサーバ装置とは独立したチケットサーバ装置で行うことによって、情報の提供時にストリーミングシステムのパフォーマンスを低下させることなく、利用者認証処理や課金処理を安全に行うことが可能となる。

【0035】さらに、情報の販売者とストリーミングシステムの運用者との間の合意に基づいてそれぞれの送信規約を作成し、それそれが運用するチケットサーバ装置とストリーミングサーバ装置とで個別に管理することによって、情報の販売者とストリーミングシステムの運用者との間で公正な利益分配を行なうことが可能となる。

【0036】
【発明の実施の形態】次に、本発明の実施例について図面を参照して説明する。図1は本発明の一実施例による情報販売システムの構成を示すブロック図である。図1において、本発明の一実施例による情報販売システムは情報を提供する情報提供装置であるストリーミングサーバ装置1と、チケットを提供するチケット提供装置であるチケットサーバ装置2と、提供された情報を再生する再生装置3とから構成されている。

【0037】ストリーミングサーバ装置1は情報提供手

50

段11と、第1の送信規約管理手段12と、パケット生成手段13と、情報蓄積手段14と、各手段で実行されるプログラムを格納する記録媒体15とから構成されている。

【0038】情報提供手段11は再生装置3から受信した情報提供要求メッセージ中に記載された情報識別子をパケット生成手段13に伝達し、パケット生成手段13から取得されるパケットあるいはエラーメッセージを再生装置3に送信する。

【0039】第1の送信規約管理手段12は1者以上の情報の販売者から与えられた全ての第1の送信規約を保持しており、パケット生成手段13から情報識別子の入力を受けた時、それに対応する第1の送信規約に記載された情報暗号鍵をパケット生成手段13に出力するか、あるいはエラーメッセージをパケット生成手段13に出力する。ここで、第1の送信規約は提供する情報を暗号化するための情報暗号鍵とユーザに対する販売条件(送信タイミング、有効期間、課金条件等)とを少なくとも含んでいる。

【0040】パケット生成手段13は情報提供手段11からユーザに提供すべき情報を識別するための情報識別子の入力を受けると、その情報識別子を第1の送信規約管理手段12に入力し、その情報に対応する情報暗号鍵を取得するか、エラーメッセージを取得する。また、パケット生成手段13はこの情報識別子を情報蓄積手段14に入力し、ユーザに提供すべき情報を取得する。さらに、パケット生成手段13はその情報とそれに対応する情報暗号鍵とから生成したセキュアパケットを廟に情報提供手段11に出力するか、あるいはエラーメッセージを情報提供手段11に出力する。

【0041】情報蓄積手段14は1者以上の情報の販売者から与えられた全ての情報を保持しており、パケット生成手段13から情報識別子の入力を受けた時、それに対応する情報をパケット生成手段13に出力する。

【0042】チケットサーバ装置2はチケット提供手段21と、第2の送信規約管理手段22と、チケット生成手段23と、第2のアカウント管理手段24と、課金手段25と、各手段で実行されるプログラムを格納する記録媒体26とから構成されている。

【0043】チケット提供手段21は再生装置3から受信したチケット要求メッセージをチケット生成手段23に伝達し、チケット生成手段23から取得したチケットを再生装置3に送信するか、あるいはエラーメッセージを再生装置3に送信する。ここで、チケットには再生装置3から要求される情報を復号して再生可能とするための情報復号鍵や上記の販売条件等を少なくとも含んでいる。

【0044】第2の送信規約管理手段22は1つ以上の第2の送信規約を保持しており、チケット生成手段23からチケットが要求された情報を識別するための情報識

別子の入力を受けると、それに対応する第2の送信規約をチケット生成手段23に出力する。ここで、第2の送信規約には情報復号鍵と上記の販売条件とを少なくとも含んでいる。

【0045】チケット生成手段23はチケット提供手段21からチケット要求メッセージの入力を受けると、そのチケット要求メッセージを第2の送信規約管理手段22に伝達し、そのチケット要求メッセージに応する第2の送信規約を取得する。また、チケット生成手段23は当該チケット要求メッセージ内に記載されたクライアント情報及び第2の送信規約を第2のアカウント管理手段24に伝達し、利用可否メッセージを取得する。さらに、チケット生成手段23は生成したチケットチケット提供手段21に出力するか、あるいはエラーメッセージをチケット提供手段21に出力する。

【0046】ここで、クライアント情報にはチケット要求メッセージを送ってきたユーザに対する認証処理や課金処理を行うために、ユーザを特定するための利用者情報やそのユーザが使用する端末装置を特定するための使用装置情報を含んでいる。

【0047】第2のアカウント管理手段24はチケットサーバ装置2でサポートするユーザもしくはホストに対する1つ以上のアカウントを保持しており、チケット生成手段23からクライアント情報及び第2の送信規約の入力を受けた時、対応するアカウントの有無やその他の条件判定の結果等に応じて生成された利用可否メッセージをチケット生成手段23に出力する。また、第2のアカウント管理手段24は必要に応じて課金情報を課金手段25に出力する。課金手段25は第2のアカウント管理手段24から課金情報の入力を受けると、適切な課金処理を行。

【0048】再生装置3は端末入力手段31と、情報要求手段32と、パケット受信手段33と、情報再生手段34と、端末出力手段35と、チケット受信手段36と、第1のアカウント管理手段37と、各手段で実行されるプログラムを格納する記録媒体38とから構成されている。

【0049】端末入力手段31はユーザからの入力を受けるためのキーボード装置や、マウス装置等の入力デバイスを備え、その入力デバイスからの入力データを適切に解釈し、チケット受信開始メッセージをチケット受信手段36に出力する。また、端末入力手段31は情報受信開始メッセージを情報要求手段32に出力する。

【0050】情報要求手段32は端末入力手段31から情報受信開始メッセージの入力を受けると、その情報受信開始メッセージ内に記載されたストリーミングサーバのURL(Universal Resource Locator)等を基に適切なストリーミングサーバ装置1との間のコネクションを確立し、ストリーミングサーバ装置1に情報要求メッセージを送信する。

【0051】パケット受信手段3-3はストリーミングサーバ装置1からセキュアパケットを受信した際、チケット受信手段3-6から入力された情報復号鍵を用いてそのセキュアパケットを復元した結果(復元パケット)を情報再生手段3-4に出力する。情報再生手段3-4はパケット受信手段3-3から復元パケットの入力を受けると、適切な復元処理によって得られる再生データを端末出力手段3-5に出力する。

【0052】端末出力手段3-5はユーザに情報を適切に提示するためのモニタ装置やスピーカ装置、及びミキサ装置等の出力デバイスを備えており、情報再生手段3-4から再生データの入力を受けると、その再生データを出力デバイスに出力する。

【0053】チケット受信手段3-6は端末入力手段3-1からチケット受信開始メッセージの入力を受けた際、第1のアカウント管理手段3-6からクライアント情報を取得する。また、チケット受信手段3-6はチケット受信開始メッセージ内に記載されたチケットサーバのURLを基に、適切なチケットサーバ装置2との間のコネクションを確立し、そのチケットサーバ装置2にチケット要求メッセージを送信する。

【0054】第1のアカウント管理手段3-7はユーザID(識別情報)やパスワード等の利用者情報を含むクライアント情報を保持しており、チケット受信手段3-6からの要求に応じてクライアント情報をチケット受信手段3-6に出力する。

【0055】図2は本発明の一実施例による情報販売システムの動作を示すフローチャートであり、図3は図2のチケット要求処理を示すフローチャートであり、図4は図2のチケット要求確認処理を示すフローチャートである。

【0056】図5は本発明の一実施例における送信規約管理表の一例を示す図であり、図6は本発明の一実施例における送信規約の一例を示す図であり、図7は本発明の一実施例におけるアカウント管理表の一例を示す図である。

【0057】図8は図1のチケットサーバ装置2における決済センタへクライアント情報の正当性確認を委譲するための構成の一例を示す図であり、図9は図2の課金処理を示すフローチャートであり、図10は図1のチケットサーバ装置2における決済センタを用いて課金処理を行うための構成の一例を示す図である。

【0058】図11は図2のチケット生成処理を示すフローチャートであり、図12は本発明の一実施例におけるチケットのフォーマットの一例を示す図であり、図13は図2のチケット受信処理を示すフローチャートであり、図14は図2の情報要求処理を示すフローチャートである。

【0059】図15は図2の情報抽出処理を示すフローチャートであり、図16は本発明の一実施例における情

報管埋表の一例を示す図であり、図17は図2のパケット送出処理を示すフローチャートであり、図18は図2の情報再生処理を示すフローチャートである。

【0060】これら図1～図18を参照して本発明の一実施例による情報販売システムの動作について説明する。尚、上記の図2～図4、図9、図11、図13～図15、図17、図18に示す処理はストリーミングサーバ装置1、チケットサーバ装置2、再生装置3各々の各手段が記録媒体1-5、2-6、3-8に夫々格納されたプログラムを実行することで実現される。

【0061】本発明の一実施例による情報販売システムにおいて、まず、再生装置3はユーザ入力解釈処理を行う(図2ステップA3-1)。具体的には、再生装置3の端末入力手段3-1において、ユーザから情報識別子とストリーミングサーバ装置1の位置情報とチケットサーバ装置2の位置情報に関する入力を受ける。

【0062】このような入力方法の好適な例としては、ストリーミングサーバ装置1上の情報を特定するためのURLと、チケットサーバ装置2上の情報を対応した送信規約を特定するためのURLとを、キーボードから入力させる方法がある。また、これら2つのURLを含むようなメタファイルを用いてもよい。特に、メタファイルを利用する場合、再生装置3の端末入力手段3-1にはメタファイルの蓄積や読み込みを行うハードディスク装置等の2次記憶装置と、その2次記憶装置上のファイルを指示するため的一般に良く知られたU1(User Interface)手段とを備えればよい。さらに、2次記憶装置の代わりにメモリカード等の補助記憶装置を用いてもよい。

【0063】その後に、再生装置3はチケット要求処理を行う(図2ステップS3-2)。具体的には、図3を参照すると、まず、端末入力手段3-1においてはステップA3-1で得られたユーザ入力解釈結果のうち、少なくとも情報識別子とチケットサーバ装置2の位置情報を含んだチケット受信開始メッセージを生成する(図3ステップS1)。

【0064】このチケット受信開始メッセージがチケット受信手段3-6に伝達された後、チケット受信手段3-6においては第1のアカウント管理手段3-7からクライアント情報を取得する(図3ステップS2)。ここで、第1のアカウント管理手段3-7は暗号ファイルシステム等を用いて安全に保護された2次記憶装置、またはセキュアメモリカード等の補助記憶装置によって構成されており、第1のアカウント管理手段3-7で保持されるクライアント情報はチケットサーバ装置2における課金処理のために必要な情報、例えばユーザIDまたはパスワードや、ユーザの公開鍵証明書等を含む。

【0065】チケット受信手段3-6はチケット受信開始メッセージ内の情報識別子と、ストリーミングサーバ装置1の位置情報と、チケットサーバ装置2の位置情報

と、クライアント情報とを含むチケット要求メッセージを生成した後(図3ステップS3)、チケットサーバ装置2の位置情報[例えば、IP(Internet Protocol)アドレスやホスト名]を基にチケットサーバ装置2との通信を確立し、チケット要求メッセージを送信する(図3ステップS4)。

【0066】チケットサーバ装置2では、まずステップA3で再生装置3から送信されたチケット要求に対する受信処理を行う(図2ステップA21)。より詳細には、図4を参照すると、チケット提供手段21においては、まずチケット要求メッセージを受信し、そのメッセージをチケット生成手段22に入力する(図4ステップS11)。

【0067】チケット生成手段23においてはチケット要求メッセージ内に記載された情報識別子を抽出して第2の送信規約管理手段24に入力し、対応する第2の送信規約またはエラーメッセージを取得する(図4ステップS12)。その際、第2の送信規約管理手段24はその内部に第2の送信規約管理表(図示せず)を備えている。

【0068】この第2の送信規約管理表は、例えば、図5に示すように、情報識別子をインデックスとして各第2の送信規約の実体の参照／読み込みが行えるようになっている。また、情報識別子に合致するようなインデックスがあった時には、対応する第2の送信規約をチケット生成手段23に派出し、合致するものがなければエラーメッセージを派出するようになっている。ここで、第2の送信規約には、例えば、図6に示すように、情報復号鍵や課金額等が含まれる。

【0069】チケット生成手段23は第2の送信規約管理手段24からの出力を確認し、その出力が第2の送信規約であるか、エラーメッセージであるかを判定する(図4ステップS13)。エラーメッセージであった場合、チケット生成手段23は不正なチケット要求である旨を伝えるエラーチケットを生成して再生装置3へ送信し、以降の処理を中断する(図4ステップS14)。

【0070】一方、第2の送信規約であった場合、チケット生成手段23はチケット要求メッセージに含まれるクライアント情報を抽出し、第2のアカウント管理手段24に入力してそのクライアント情報の正当性を確認する(図4ステップS15)。

【0071】ここで、第2のアカウント管理手段24におけるクライアント情報の正当性の確認方法について、好適な一例としては、クライアント情報として課金処理可能なユーザIDとパスワードとの組を用いた場合等において、図7に示すように、予め登録済みの全クライアント情報を記録したアカウント管理表を作成しておく方法がある。この方法の場合には、クライアント情報の入力に応じてアカウント管理表内に合致するものを検索するようにし、合致するものがあれば正当であるとし、ま

たは合致するものがなければ不正であると判定する。

【0072】あるいは、他の好適な例として、クレジットカードやプリペイドカード等の認証に必要な情報(会員番号やカードID等)をクライアント情報として用いる方法もある。この方法の場合には、上記のようなアカウント管理表は必ずしも必須ではなく、むしろ、図8に示すように、第2のアカウント管理手段24と決済センタ4とをネットワークで結び、第2のアカウント管理手段24に入力されたクライアント情報の正当性確認処理を決済センタ4に委託してもよい。

【0073】このようにして、クライアント情報の正当性を確認した後、不正なクライアント情報であると判定された場合には、不正なクライアント情報を含む旨を伝えるエラーチケットを生成して再生装置3へ送信し、以降の処理を中断する(図4ステップS16)。一方、正当なクライアント情報であると判定された場合には、次のステップへと処理を移行する。

【0074】続いて、チケットサーバ装置2は課金処理を行う(図2ステップA22)。より詳細には、図9を参照すると、まず、チケット生成手段23においては送信規約から課金額を取得する(図9ステップS21)。第2のアカウント管理手段24は少なくとも課金額とクライアント情報を課金手段25に入力し、適切な課金を行う(図9ステップS22)。

【0075】課金ログ等を残したい時には、この他に、情報識別子等、任意の情報を入力してよい。この際に用いる課金システムは、上述したように、ユーザIDとパスワードとの組をクライアント情報として扱う場合、いわゆる会員制課金システムとして動作させればよい。つまり、予めユーザの決済口座を登録しておき、決済口座に一意に対応するユーザIDとパスワードとの組を発行しておき、課金手段25において、当該ユーザID及びパスワードの組と、課金額とが入力された際に、決済口座宛ての請求書を生成すれば、オンラインで決済することができる。

【0076】もちろん、金融機関がネットワーク上の決済サーバを持つ場合、例えば、上述したようなクレジットカードやプリペイドカードを用いる場合には、図10に示すように、課金手段25と決済サーバ4とをネットワークで結び、クライアント情報と課金額とを決済サーバ4に送信することで、オンライン決済也可能となる。

【0077】次に、チケットサーバ装置2はチケット生成処理を行う(図2ステップA23)。より詳細には、図11を参照すると、少なくとも送信規約に記載された情報復号鍵を含む、例えば、図12に示すようなチケット基底データを生成し(図11ステップS31)、チケット基底データに対してチケットの正当性証明や再生装置3のユーザ以外の第三者からの参照を防ぐためのセキュリティ的な保護を施したものチケットとする(図11ステップS32)。

【0078】この際、セキュリティ保護の具体的方法として、好適な一例を示すと、まず、チケット生成手段2 3内にチケットサーバ装置2の公開鍵証明書を保持しておき、その公開鍵証明書を用いてチケット基底データにデジタル署名を加える。あるいは、再生装置3のユーザにのみ参照可能なようにチケット基底データに暗号化を施す。この際、暗号化に用いる鍵としては、再生装置3の第1のアカウント管理手段3 7で保持された特定の鍵をチケット要求メッセージ内に記載しておくか、第2のアカウント管理手段2 4におけるクライアント情報の一部として予め登録しておいたものを用いればよい。もちろん、その鍵はチケットサーバ装置2と再生装置3との間で共通のものでもよいし、RSA (R i v e s t S h a m i n g A d l e m a n) 等の公開鍵暗号系における公開鍵／秘密鍵といった鍵ペアでもよい。

【0079】その後、上記のようして生成されたチケットはチケット生成手段2 3からチケット提供手段2 1へと送られ、チケット提供手段2 1から再生装置3へ送信される(図2ステップA 2 4)。

【0080】再生装置3はチケットサーバ装置2からのチケットに対するチケット受信処理を行う(図2ステップA 3 3)。より詳細には、図1 3を参考すると、再生装置3のチケット受信手段3 6においてはチケットサーバ装置2から受信したチケットに対してセキュリティ保護を解除する(図1 3ステップS 4 1)。例えば、上記のチケット生成処理に記述したように、チケットが再生装置3を使用するユーザのみに参照し得るよう暗号化が施されている場合、第1のアカウント管理手段3 7に保持された再生装置3に固有の鍵で復号する。あるいは、チケットサーバ装置2の公開鍵証明書を用いてチケットに施されたデジタル署名を確認することによって、チケットの正当性を検証することができる。

【0081】再生装置3は上記のチケットからチケット基底データを抽出し(図1 3ステップS 4 2)、チケット基底データに記載されている情報復号鍵をパケット受信手段3 3へ入力し、パケット受信手段3 3にてその情報復号鍵を保持する(図1 3ステップS 4 3)。

【0082】この後に、再生装置3は情報要求処理を行う(図2ステップA 3 4)。より詳細には、図1 4を参考すると、端末入力手段3 1においては少なくとも情報識別子とストリーミングサーバ装置1の位置情報とを含む情報要求開始メッセージが生成され、情報要求手段3 2に入力される(図1 4ステップS 5 1)。

【0083】情報要求手段3 2は少なくとも情報識別子を含む情報要求メッセージを生成し(図1 4ステップS 5 2)、ストリーミングサーバ装置1の位置情報に対応する適切なストリーミングサーバ装置1との通信を確立した後、情報要求メッセージをストリーミングサーバ装置1へ送信する(図1 4ステップS 5 3)。この時、その情報要求メッセージを第三者に覗き見されないよう

に、例えばSSL等の暗号通信方式を用いることもできるが、その方式は必須ではない。

【0084】ストリーミングサーバ装置1は再生装置3から情報要求メッセージが送られてくると、情報要求確認処理を行う(図2ステップA 1 1)。具体的に、ストリーミングサーバ装置1の情報提供手段1 1においては再生装置3から受信した情報要求メッセージを解釈し、情報識別子を抽出した後、パケット生成手段1 3へ入力する。この際、上記のように、情報要求メッセージが暗号化されていれば、解釈処理の前に復号処理を行っておく。

【0085】続いて、ストリーミングサーバ装置1は情報抽出処理を行う(図2ステップA 1 2)。より詳細には、図1 5を参考すると、パケット生成手段1 3においては情報識別子を第1の送信規約管理手段1 2へ入力し、対応する送信規約またはエラーメッセージを取得する(図1 5ステップS 6 1)。この時、第1の送信規約管理手段1 2は、例えば、その内部に第1の送信規約管理表(図示せず)を備えている。

【0086】第1の送信規約管理表は、上述した第2の送信規約管理表と同様な構造を持ち、情報識別子をインデックスとして、各第1の送信規約の実体の参照／読み込みが行えるようになっている。第1の送信規約管理手段1 2は情報識別子に合致するようなインデックスがあれは対応する第1の送信規約をパケット生成手段1 3に出力し、合致するものがなければエラーメッセージをパケット生成手段1 3に出力するようになっている。また、第1の送信規約はチケットサーバ装置2の第2の送信規約管理手段2 2における第2の送信規約と全く同一でなくともよく、少なくとも情報暗号鍵を含んでいれば十分である。

【0087】その後、パケット生成手段1 3は第1の送信規約管理手段1 2からの出力が第1の送信規約であるか、エラーメッセージであるかを判定する(図1 5ステップS 6 2)。エラーメッセージであった場合、パケット生成手段1 3は、例えば、ストリーミングサーバ装置2上で適切な情報がサポートされない旨を伝えるようなエラーメッセージを新たに生成し、情報提供手段1 1を介して再生装置3へ送信し、以降の処理を中断する(図1 5ステップS 6 6)。

【0088】一方、第1の送信規約であった場合、パケット生成手段1 3は第1の送信規約から情報暗号鍵を抽出し、一時保持しておく(図1 5ステップS 6 3)。パケット生成手段1 3は情報識別子を情報蓄積手段1 4に入力し、対応する情報を取得する(図1 5ステップS 6 4)。

【0089】この時、情報蓄積手段1 4は、例えば、その内部に、図1 6に示すような情報管理表を保持しており、情報識別子をインデックスとして、動画データや音声データのようなユーザに提供すべき情報の参照／読み込

みを行えるようになっている。ユーザに提供すべき情報のフォーマットはMPEG2(Moving Picture Experts Group 2)やMP3(MPEG audio layer 3)等の任意のものでよく、少なくとも動画フレームや固定長レコード等といった「断片」の系列として、順にアクセス可能であれば十分である。

【0090】次に、ストリーミングサーバ装置1はパケット送出処理を行う(図2ステップA13)。より詳細には、図17を参照すると、パケット生成手段13においては情報蓄積手段14から上記のような情報の断片を読みながら、その断片を含んだパケットを生成する(図17ステップS71)。パケットは上記の断片の他に、パケットの順番を示すシリアル番号等が付加された、例えばRFC(Request For Comments)2250に記載されているようなRTP(Real-time Transport Protocol)ペイロード等と同様的一般的な構造を持つ。

【0091】パケット生成手段13はそうして生成されたパケットに対して、保持しておいた情報暗号鍵を用いて暗号化してセキュアパケットを生成する(図17ステップS72)。パケット生成手段13はセキュアパケットを順次、情報提供手段11を介して再生装置3へ送信する(図17ステップS73)。

【0092】パケット生成手段13はこれら一連の処理(図17ステップS71～S73)を、情報蓄積手段14から上記のような情報の断片を読み終えるまで繰り返し行う(図17ステップS71～S74)。パケット生成手段13は情報蓄積手段14から上記のような情報の断片を読み終えた時に情報送信完了メッセージを生成し、情報提供手段11を介して再生装置3へ送信する(図17ステップS75)。

【0093】再生装置3はストリーミングサーバ装置1から情報送信完了メッセージが送られてくると、情報再生処理を行う(図2ステップA35)。より詳細には、図18を参照すると、まず、再生装置3のパケット受信手段33においてはストリーミングサーバ装置1の情報提供手段11からのデータが受信される度に、そのデータがセキュアパケットか否かを判定する(図18ステップS81)。

【0094】パケット受信手段33はセキュアパケットを受信すると、上記のステップA33で保持しておいた情報復号鍵を用いて復号していく(図18ステップS82)、復号後に得られるパケットを情報再生手段34へ入力する。情報再生手段34では入力されたパケットを、パケットに付加されたシリアル番号等を基に情報の一部分を適切に連結し、元の動画データや音声データ等の情報を復元し(図18ステップS83)、端末出力手段35を介してユーザにその復元した情報を提示し(図18ステップS84)、ステップS81に戻る。

【0095】一方、ストリーミングサーバ装置1の情報提供手段11から受信されたデータが各種エラーメッセージであるか、情報送信完了メッセージである場合、パケット受信手段33は情報再生処理を中断し、適切な終了処理を行なう(図18ステップS85)。この終了処理の好適な一例としては、エラーメッセージを受信した場合に、そのエラー内容をユーザに伝えるための警告ダイアログを端末出力手段35を介して表示する方法や、情報送信完了メッセージを受信した場合に、端末出力手段35に表示されていた動画表示用のウィンドウを閉じて再生装置3の初期化を行う方法がある。

【0096】このように、本実施例では、通常、ストリーミング通信を用いた情報販売システムにおけるストリーミングサーバ装置1と再生装置3とに加えて、チケットサーバ装置2を持つように構成しているため、ストリーミングサーバ装置1はユーザ認証処理や課金処理を行う必要がなくなり、販売におけるセキュリティを保ちながら、その応答性能を最大化することができる。

【0097】また、情報要求処理(図2ステップA34)において、再生装置3からストリーミングサーバ装置1へ伝達される情報要求メッセージには、チケット要求処理(図2ステップA32)におけるチケット要求メッセージと異なり、ユーザを特定したり、課金に必要となるようなクライアント情報が含まれない。こうすることで、チケットサーバ装置2を管理する情報の販売者は、顧客であるユーザのプライバシを厳格に保護することができる。

【0098】さらに、ストリーミングサーバ装置1が実際に複数台のホスト上で動作している場合でも、チケットサーバ装置2は少なくとも1台のホストで動作していればよいため、情報販売システム全体のスケーラビリティの向上に寄与とともに、情報の販売者は複数のストリーミングシステムの運用者に情報配信処理を委託することができる。

【0099】さらにまた、逆に、1台のストリーミングサーバ装置1について、チケットサーバ装置2が実際に複数台のホスト上で動作することも可能であるため、ストリーミングシステムの運用者は複数の情報の販売者から情報配信処理の委託を受けることができる。

【0100】尚、上記の説明では再生装置3において断片化された情報の受信及び再生を並列的に行なうストリーミングデータを販売する場合について述べているが、プログラムや静止画像データ等の販売や貸与等にも適用することができる。その場合、プログラムの販売や貸与等であれば、ストリーミングサーバ装置1の代わりにアプリケーションサーバ等を配置すればよい。

【0101】図19は本発明の一実施例による情報販売システムの具体例を示すブロック図である。図19において、本発明の一実施例による情報販売システムではチケットサーバ装置2を運用する情報の販売者P2と、ス

ストリーミングサーバ装置1を運用するストリーミングシステム運用者P1との間で、情報配信処理の委託契約を結び、再生装置3を用いる任意のユーザP3と情報の販売者P1との間で、情報の購入契約を結ぶ。

【0102】その後、ユーザP3が再生装置3及びストリーミングサーバ装置1を介して、ストリーミングシステム運用者P1から情報の提供を受ける時、チケットサーバ装置2からチケットを取得し、それと引き換えに情報の販売者P2に対してその情報の代金が支払われ、情報の販売者P2はストリーミングシステム運用者P1に対して、委託契約に基づく配信手数料を支払う。

【0103】図20は図19の情報販売システムにおける情報販売手続きを示すフローチャートであり、図21は図19のチケットサーバ装置2において課金履歴に基いて課金処理を行うための構成の一例を示すプロック図である。これら図19及び図20を参照して図19の情報販売システムにおける情報配信処理の委託契約及び配信手数料の授受を含む情報の販売方法について説明する。

【0104】まず、情報の販売者P2は任意のストリーミングシステム運用者P1と、情報の配信手数料の取り決めを行なう(図20ステップB1)。この取り決めの内容は個々の情報について異なってもよいし、配信処理1回あたりの料金を定めてよいし、特定の有効期間を定めるものでもよいし、あるいはこれらの組み合わせでもよい。

【0105】例えば、「配信処理1回あたり50円を、情報の販売者から、ストリーミングシステムの運用者に支払う。但し、動画Aについては、特別に30円/回とする」という内容でもよいし、「2001年8月1日より3ヶ月間、配信を行うものとし、情報の販売者P2から、ストリーミングシステム運用者P1に対して、配信手数料として、1000万円支払う。」というような内容でもよい。

【0106】上記のような委託契約を交わした後、情報の販売者P2は、販売の対象となる情報とそれに対応する送信規約とをストリーミングシステム運用者P1に渡す(図20ステップB2)。同時に、その送信規約にユーザP3から徴収すべき代金(課金額)等の情報を加えたものをチケットサーバ装置2の第2の送信規約管理手段22に登録しておく(図20ステップB3)。

【0107】ストリーミングシステム運用者P1は情報の販売者P2から受取った情報を、ストリーミングサーバ装置1の情報蓄積部14に登録し、さらに送信規約を第1の送信規約管理手段12に登録する(図20ステップB4)。

【0108】このようにして、委託契約とそれに伴うシステム設定を行なった後、情報の販売者P2は情報に対応する情報識別子と、ストリーミングサーバ装置1の位置情報と、チケットサーバ装置2の位置情報を含む

だ、例えばメタファイルを作成する(図20ステップB5)。情報の販売者P2はそのメタファイルを要求するユーザP3があれば、このユーザP3との間で、販売(購入)契約を結ぶ(図20ステップB6)。

【0109】販売契約を結ぶにあたっては情報の代金が情報の販売者P2からユーザP3に提示され、その決済に必要な情報をユーザP3が情報の販売者P2に返す。この時、決済に必要な情報として、クレジットカードの会員番号や、銀行口座の番号等を逐一入力する形態でもよいし、情報の販売者P2によって予め用意されたWebシステム等において、そうした決済用情報をユーザIDやパスワード等とともに登録しておき、各購入契約にあたってはユーザIDやパスワードを入力するという形態でもよい。いずれの形態においても、決済用情報と、もしあればそれに関連付けられたユーザID等の情報をチケットサーバ装置2のアカウント管理手段24に登録しておく。

【0110】ユーザP3と情報の販売者P2との間で販売契約が成立した後、メタファイルがユーザP3に配布される(図20ステップB7)。その後、このメタファイルが再生装置3に入力されると、再生装置3はメタファイルに記述されたストリーミングサーバ装置1及びチケットサーバ装置2との間で、上述したステップA31～A35までの動作を行い、情報の提供を受ける(図20ステップB8)。

【0111】この時、特にチケット要求処理(図2ステップA32)において、チケット要求メッセージには決済用情報に関連付けから得たユーザIDもしくは決済用情報そのものであるクレジットカード会員番号等がクライアント情報の一部として含まれ、課金処理(図2ステップA22)において、当該ユーザID等に関連付けられた決済用情報あるいはチケット要求メッセージに含まれる決済用情報そのものに基づいて課金処理が行われる。ユーザID等を用いる場合には上記のステップB6において、アカウント管理手段24で関連付けられた決済用情報が登録されているので、これを用いればよい。

【0112】その後、情報の販売者P2はストリーミングシステムの運用者P1に、上記のステップB1で交わした契約に基づいて、所定の配信手数料を支払う(図20ステップB9)。特に、情報の配信処理1回毎に手数料が発生するような契約形態である場合には、チケットサーバ装置2の課金手段25における課金処理(図2ステップA22)のログデータを基に、一定期間内の配信手数料を算出することができる。

【0113】このため、図21に示すように、課金手段25と情報の販売者P2が別途用意した課金ログデータベース5とを接続しておき、課金処理(図2ステップA22)の処理時に、少なくとも情報識別子と課金額とが課金ログデータベース5に蓄積されるようにしておけばよい。

【0114】上記のステップB1で交わした契約に、期間等の契約失效の条件がある場合、失效時に上記のステップB3でチケットサーバ装置2の送信規約管理部23に登録した第2の送信規約を削除することで、情報の販売者P1による契約解除を行うことができる。

【0115】図22は本発明の他の実施例による情報販売システムの構成を示すブロック図である。図22において、本発明の他の実施例による情報販売システムはチケットサーバ装置2に代えて第2のチケットサーバ装置6を備えた以外は図1に示す本発明の一実施例による情報販売システムと同様の構成となっており、同一構成要素には同一符号を付してある。また、同一構成要素の動作は本発明の一実施例と同様である。つまり、図示していないが、ストリーミングサーバ装置1及び再生装置3の構成は図1に示すストリーミングサーバ装置1及び再生装置3の構成と同じである。

【0116】第2のチケットサーバ装置6は、図1に示すチケットサーバ装置2と比較して、第2の送信規約管理手段22に代えて、送信規約グループ管理手段61と、N個の第2の送信規約管理手段2-1～2-Nとを備える点で異なる。尚、記録媒体26には送信規約グループ管理手段61と、N個の第2の送信規約管理手段2-1～2-Nにおいてそれぞれ実行されるプログラムも格納されているものとする。

【0117】送信規約グループ管理手段61はチケット生成手段23から少なくとも第2の情報識別子の入力を受け、適切な第2の送信規約管理手段（例えば、第k番目の第2の送信規約管理手段22-k）を選択し、選択した第2の送信規約管理手段22-kへ情報識別子を人力し、その応答として得られた第2の送信規約もしくはエラーメッセージをチケット生成手段23へ出力する。

【0118】また、それぞれの第2の送信規約管理手段2-1～2-Nは送信規約グループ管理手段61から情報識別子の入力を受けて、図1に示す第2の送信規約管理手段22と同様にして、その情報識別子に対応する第2の送信規約を検索し、検索した第2の送信規約を送信規約グループ管理手段61へ出力する。

【0119】図23は本発明の他の実施例による情報販売システムの動作を示すフローチャートであり、図24は図23の第2のチケット要求確認処理を示すフローチャートであり、図25は本発明の他の実施例における第2の情報識別子のフォーマットの一例を示す図であり、図26は本発明の他の実施例における送信規約グループ管理表の一例を示す図である。

【0120】これら図22～図26を参照して本発明の他の実施例による情報販売システムの動作について説明する。尚、図23及び図24に示す処理はストリーミングサーバ装置1、第2のチケットサーバ装置6、再生装置3各々の各手段が記録媒体15、26、38に夫々格納されたプログラムを実行することで実現される。

【0121】ここで、図23に示す第2のチケットサーバ装置6の動作は、図2に示すチケットサーバ装置2の動作におけるチケット確認処理（図2ステップA21）の代わりに、第2のチケット確認処理（図23ステップA71）を行うようにした点で本発明の一実施例による情報販売システムと異なる。

【0122】ステップA71をより詳細に述べると、図24に示すように、まず、図2のチケット確認処理（図2ステップA21）と同様に、第2のチケットサーバ装置6においてはチケット提供手段21で受信したチケット要求がチケット生成手段23に伝達される（図24ステップS91）。

【0123】その後、チケット生成手段23はチケット要求に記載された第2の情報識別子を抽出して送信規約グループ管理手段61へ入力する（図24ステップS92）。送信規約グループ管理手段61は第2の情報識別子を運用者識別子と情報識別子（第1の情報識別子）（本発明の一実施例におけるものと同一）とに分割する（図24ステップS93）。

【0124】送信規約グループ管理手段61は運用者識別子から適切なk番目の第2の送信規約管理手段22-kを選択し、第1の情報識別子を第2の送信規約管理手段22-kに入力し、第2の送信規約もしくはエラーメッセージを取得し、チケット生成手段23へ出力する（図24ステップS94）。

【0125】この後、チケット生成手段23は、上述した本発明の一実施例と同様に、第2の送信規約かエラーメッセージかの判定（図24ステップS95）と、エラー処理（図24ステップS96）もしくはチケット要求の正当性確認（図24ステップS96）を行う。

【0126】尚、第2の情報識別子は、図25に示すように、予めストリーミングシステム運用者毎に定められた運用者識別子（例えば、ストリーミングシステム運用者のドメイン名等）と、第1の情報識別子を連結したフォーマットを持っており、再生装置3及びストリーミングサーバ装置1においては第1の情報識別子と全く同様に扱われる。また、送信規約グループ管理手段61はその内部に、図26に示すように、運用者識別子とそれに応対する第2の送信規約管理手段22-kとの関連付け（例えば、ボイント）を保持する表を保持している。

【0127】このように、情報の販売者が複数のストリーミングシステム運用者に対して、委託契約を結ぶ際に、ストリーミングシステム運用者毎に異なる契約内容を持たせたり、あるいは異なる情報の委託及び管理を行うことができる。

【0128】図27は本発明の別の実施例による情報販売システムの構成を示すブロック図である。図27において、本発明の別の実施例による情報販売システムはストリーミングサーバ装置1に代えて第2のストリーミングサーバ装置7を備え、再生装置3に代えて第2の再生

装置8を備えるようにした以外は図1に示す本発明の一実施例による情報販売システムと同様であり、同一構成要素には同一符号を付してある。また、同一構成要素の動作は本発明の一実施例と同様である。つまり、図示していないが、チケットサーバ装置2の構成は図1に示すチケットサーバ装置2の構成と同じである。

【0129】第2のストリーミングサーバ装置7は第1のセッション鍵確立手段71を設け、パケット生成手段13に代えて第2のパケット生成手段72を設けた以外は図1に示すストリーミングサーバ装置1と同様の構成である。尚、記録媒体15には第1のセッション鍵確立手段71と、第2のパケット生成手段72においてそれぞれ実行されるプログラムも格納されているものとする。

【0130】第1のセッション鍵確立手段71は第2の再生装置8からのセッション鍵要求メッセージを受信すると、適当なセッション鍵を発生して保持し、そのセッション鍵を第2の再生装置8に送信する。また、第1のセッション鍵確立手段71は第2のパケット生成手段72からの要求に応じて、そのセッション鍵を第2のパケット生成手段72に送出する。ここで、セッション鍵とは情報暗号鍵を変形するための情報を示しており、例えば、乱数やワンタイムパスワード等がある。すなわち、セッション鍵は第2の再生装置8との間のセッション毎に使用される使い捨ての鍵情報である。

【0131】第2のパケット生成手段72は情報提供手段11から情報識別子の入力を受けると、その情報識別子を基に情報暗号鍵を取得するか、あるいはエラーメッセージを取得する。また、第2のパケット生成手段72は情報識別子を情報蓄積手段14に入力し、ユーザに提供すべき情報を取得する。

【0132】さらに、第2のパケット生成手段72は第1のセッション鍵確立手段71からセッション鍵を取得し、そのセッション鍵を情報暗号鍵と統合する。さらにもう、第2のパケット生成手段72は情報と、統合された情報暗号鍵とから生成したセキュアパケットを順に情報提供手段11に出力するか、あるいはエラーメッセージを情報提供手段11に出力する。

【0133】第2の再生装置8は第2のセッション鍵確立手段81を設け、パケット受信手段35に代えて第2のパケット受信手段82を設けた以外は図1に示す再生装置3と同様の構成となっている。尚、記録媒体38には第2のセッション鍵確立手段81と、第2のパケット受信手段82においてそれぞれ実行されるプログラムも格納されているものとする。

【0134】第2のセッション鍵確立手段81は第2のストリーミングサーバ装置7の第1のセッション鍵確立手段71に対してセッション鍵要求メッセージを送信し、第1のセッション鍵確立手段71からセッション鍵を受信して保持する。また、第2のセッション鍵確立手

段81は第2のパケット受信手段82からの要求に応じて、受信したセッション鍵を第2のパケット受信手段82に送出する。

【0135】第2のパケット受信手段82は第2のストリーミングサーバ装置7からセキュアパケットを受信した際、チケット受信手段36から入力された情報復号鍵と、第2のセッション鍵確立手段81から取得されるセッション鍵とを用いて、そのセキュアパケットを復元した結果（復元パケット）を情報再生手段34に出力する。

【0136】図28は本発明の別の実施例による情報販売システムの動作を示すフローチャートであり、図29は図28の第2の情報抽出処理を示すフローチャートであり、図30は図28のセッション鍵要求処理を示すフローチャートであり、図31は図28のセッション鍵生成処理を示すフローチャートである。

【0137】図32は図28のセッション鍵受信処理を示すフローチャートであり、図33は図28の第2のパケット送出処理を示すフローチャートであり、図34は図28の第2の情報再生処理を示すフローチャートである。

【0138】これら図27～図34を参照して本発明の別の実施例による情報販売システムの動作について説明する。尚、図28～図34に示す処理は第2のストリーミングサーバ装置7、チケットサーバ装置2、第2の再生装置8各々の各手段が記録媒体15、26、38に夫々格納されたプログラムを実行することで実現される。

【0139】ここで、図28において、ユーザ入力開始処理（図2ステップA31）から情報要求確認処理（図2ステップA11）までの処理は本発明の一実施例による情報販売システムと同一の処理を行う。その後、本発明の一実施例による情報販売システムの動作における情報抽出処理（図2ステップA12）の代わりに、第2の情報抽出処理（図28ステップA71）が行われ、その後、第2の再生装置8と第2のストリーミングサーバ装置7との間で、セッション鍵要求処理（図28ステップA81）と、セッション鍵生成処理（図28ステップA72）と、セッション鍵受信処理（図28ステップA82）とが行われる点で本発明の一実施例と異なる。

【0140】また、本発明の一実施例による情報販売システムの動作におけるパケット送出処理（図2ステップA13）及び情報再生処理（図2ステップA35）の代わりに、第2のパケット送出処理（図28ステップA73）と第2の情報再生処理（図28ステップA83）とが行われる点で本発明の一実施例と異なる。尚、以下の説明ではセッション鍵として乱数を用いるものとする。

【0141】まず、第2のストリーミングサーバ装置7における第2の情報抽出処理（図28ステップA71）を、図29を参照しながら、より詳細に説明すると、まず、本発明の一実施例による情報販売システムの動作と

同様の情報抽出処理(図29ステップS101～S104、S106)が行われた後、情報抽出完了メッセージを生成し、第2の再生装置8の情報要求手段32に送信する(図29ステップS105)。

【0142】その後、第2の再生装置8ではセッション鍵要求処理(図28ステップA81)が行われる。図30を参照しながら、より詳細に説明すると、情報要求手段32においては情報抽出完了メッセージを受信した際、セッション鍵確立開始メッセージを生成し、そのセッション鍵確立開始メッセージを第2のセッション鍵確立手段81に入力する(図30ステップS111)。

【0143】第2のセッション鍵確立手段81はセッション鍵要求メッセージを生成し、第2のストリーミングサーバ装置7の第1のセッション鍵確立手段71へそのセッション鍵要求メッセージを送信する(図30ステップS112)。その際、情報要求処理(図28ステップA34)で確立された通信路とは、別の通信路を用いてもよい。

【0144】第2のストリーミングサーバ装置7ではセッション鍵生成処理(図28ステップA72)が行われる。図31を参照しながら、より詳細に説明すると、第1のセッション鍵確立手段71はセッション鍵要求メッセージを受信し(図31ステップS121)、その後、乱数を生成し、それを内部的に一時保持する(図31ステップS122)。

$$\begin{aligned} F(K, R) &= K \text{ XOR } R \\ F(K, R) &= E[R] \quad (K) \\ F(K, R) &= H(K, R) \end{aligned}$$

等を用いることができる。尚、(1)式においてXORは排他的論理和を示し、(2)式においてEは乱数Rを鍵とする暗号化関数を示し、(3)式においてHは情報暗号鍵K及び乱数Rの連接を入力とする一方向性ハッシュ関数を示している。

【0149】第2のパケット生成手段72は値F(K,R)を鍵として、ステップS141で生成したパケットを暗号化し、セキュアパケットを生成する(図33ステップS144)。このようにして生成されたセキュアパケットを、順次、情報提供手段11を介して第2の再生装置8へ送信する(図33ステップS145)。

【0150】第2のパケット生成手段72はこれら一連の処理を情報の断片の読み込みが完了するまで繰り返し行い(図33ステップS141～S146)、未送出の断片が無くなつた時、情報送信完了メッセージを生成し、情報提供手段11を介して第2の再生装置8へ送信する(図33ステップS147)。

【0151】その後、第2の再生装置8で第2の情報再生処理(図28ステップA83)が行われる。図34を参照しながら、より詳細に説明すると、まず、第2のパケット受信手段82では受信データがセキュアパケットか否かの判別を行い(図34ステップS151)、もし必要ならば図1に示す再生装置3と同様に、例外処理を

*ステップS122)。第1のセッション鍵確立手段71は乱数を第2の再生装置8の第2のセッション鍵確立手段81へ送信する(図31ステップS123)。

【0145】その後、第2の再生装置8ではセッション鍵受信処理(図28ステップA82)が行われる。図32を参照しながら、より詳細に説明すると、第2のセッション鍵確立手段81は乱数を受信し(図32ステップS131)、その乱数を内部的に一時保持する(図32ステップS132)。その後、第2のセッション鍵確立手段81はセッション鍵受信完了メッセージを第1のセッション鍵確立手段71に送信する(図32ステップS133)。

【0146】第2のストリーミングサーバ装置7では第2のパケット送出処理(図28ステップA73)が行われる。図33を参照しながら、より詳細に説明すると、第2のパケット生成手段72においては、図1に示すパケット生成手段13と同様に、情報の断片の読み込みとパケット生成を行なう(図33ステップS141)。

【0147】第2のパケット生成手段72は第1のセッション鍵確立手段71から乱数Rを取得し(図33ステップS142)、保持している情報暗号鍵Kとともに、適当な統合化関数Fにかけ、その値F(K, R)に情報暗号鍵Kを置換える(図33ステップS143)。

【0148】統合化関数Fの好適な例としては、

$$\begin{aligned} \dots &\dots (1) \\ \dots &\dots (2) \\ \dots &\dots (3) \end{aligned}$$

を行って終了する(図34ステップS158)。

【0152】受信データがセキュアパケットであった場合、第2のパケット受信手段82は第2のセッション鍵確立手段81で保持されている乱数を取得する(図34ステップS152)。本発明の一実施例による動作と同様のチケット受信処理(図28ステップA33)によつて、手始め第2のパケット受信手段82で保持されている情報復号鍵Kと乱数Rとともに、統合化関数Fに掛け、その値F(K, R)に情報復号鍵Kを置換える(図34ステップS153)。

【0153】その後、第2のパケット受信手段82は値F(K, R)を用いてセキュアパケットを受信された順に復号していく(図34ステップS154)。第2のパケット受信手段82は、本発明の一実施例と同様にして、復元パケットから元の動画データや音声データ等の情報を復元し(図34ステップS155)、端末出力手段35を介してユーザにその情報を提示しながら(図34ステップS156)、ステップS151以降の処理を繰り返し行う(図34ステップS151～S157)。

【0154】このように、第2のストリーミングサーバ装置7と第2の再生装置8との間で同じ情報を提供する複数の通信(=セッション)について、セッション毎にセキュアパケットの暗号鍵及び復号鍵が異なるため、そ

のセッションを傍受する第三者に対して、より高いセキュリティを実現することができる。

【0155】尚、上記のステップA 81、A 72、A 82に記載したセッション鍵の確立に係る処理について、特に通信処理がセキュアパケットの送受信に係る通信路と異なる通信路を用いて行われる場合、セキュアパケットを複数台の第2の再生装置8に対してマルチキャスト配信することもできる。この場合、セッション鍵生成処理(図28ステップA 72)において、第2のストリーミングサーバ装置7の第1のセッション鍵確立手段71において、第2の再生装置8毎に異なる乱数を発生させることではなく、情報をマルチキャスト配信する度に異なる乱数を発生させればよい。

* 【0156】また、上記のステップA 81、A 72、A 82に記載したセッション鍵の確立に係る処理について、第2の再生装置8の第2のセッション鍵確立手段81で、乱数R2を発生させ、セッション鍵要求メッセージに乱数R2を含めることもできる。さらに、ステップA 72と同様に、第2のストリーミングサーバ装置7の第1のセッション鍵確立手段71でも乱数R1を発生させ、第2の再生装置8に送信してもよい。この場合、ステップA 73、A 83において、情報暗号鍵K1及び情報復号鍵K2を置き換えるための鍵を生成する式を、それぞれに用いればよい。

【0157】この場合の第2の統合化閑数F'及びF"

* は

$$F' (K_1, R_1, R_2) = F (K_1, DH_1 (R_1, R_2)) \dots (4)$$

$$F'' (K_2, R_1, R_2) = F (K_2, DH_2 (R_1, R_2)) \dots (5)$$

をそれぞれに用いればよい。

$$R_1 = g^r_1 \mod N \dots (6)$$

$$R_2 = g^r_2 \mod N \dots (7)$$

$$DH_1 (R_1, R_2) = (R_2)^{r_1} \mod N \dots (8)$$

$$DH_2 (R_1, R_2) = (R_1)^{r_2} \mod N \dots (9)$$

という(6)式～(9)式で示されるような閑数であり、これは、Diffie及びHellmanらによって「IEEE Transactions on Information Theory」(v. IT-22, n. 6, 1976)に記載された鍵交換法(Diffie-Hellman鍵交換法)として、一般によく知られるものである。

【0159】ここで、(6)式においてNはある大きな整数、gは整数群Z(N)上の原始元であるようなある定数、r1はある乱数、^はべき乗、modは剰余を示している。また、(7)式においてr2はある乱数を示している。こうすることで、さらに高いセキュリティを実現することができる。

【0160】このように、情報の販売者が自己の所有する情報の販売条件を送信規約として管理するためのチケットサーバ装置を備えることによって、情報の販売者がストリーミングシステムの運用者に情報の配信業務を委託する際に、情報の販売者が自己の所有する情報の販売条件を自由に設定することができる。

【0161】また、利用者認証処理や課金処理をストリーミングサーバ装置1、7とは独立したチケットサーバ装置2、6で行うことによって、情報の提供時に、ストリーミングシステムのパフォーマンスを低下させずに、利用者認証処理や課金処理を安全に行うことができる。

【0162】

【0163】

【発明の効果】以上説明したように本発明の情報販売方法は、情報を暗号化してユーザに提供するための情報暗

号鍵を含んだ第1の送信規約を管理するための第1の送信規約管理手段をストリーミングサーバ装置に設け、暗号化された情報を復号して再生可能とするための情報復号鍵を含んだ送信規約を管理するための第2の送信規約管理手段をチケットサーバ装置に設けることによって、情報の販売者とストリーミングシステムの運用者とが異なるような情報販売形態において、情報の販売者が自己の所有する情報の販売条件(価格や利用者制限)を自由に設定することができるという効果が得られる。

【0164】また、本発明の他の情報販売方法は、情報をユーザに販売するにあたって当該ユーザの認証処理を行うための第2のアカウント管理手段と、ユーザに対する課金処理を行う課金手段とをチケットサーバ装置に設け、要求された情報をユーザに送信するにあたって単に暗号化された情報の送出を行ふ情報提供手段をストリーミングサーバ装置に設けることによって、ストリーミングシステムが行う情報の送信処理のパフォーマンスを低下させることなく、利用者認証処理や課金処理を行ふことができるという効果が得られる。

【0165】さらに、本発明の別の情報販売方法は、情報の販売者が情報の代金をユーザから徴収した時に当該情報の復号鍵をユーザに与え、送信規約の一方を管理するストリーミングシステム運用者に対して所定の委託契約に基づいた配信手数料を支払うことによって、情報の販売者とストリーミングシステムの運用者とが異なるような情報販売形態において、利用者から得られる利益を、情報の販売者とストリーミングシステムの運用者との間で公正に分配することができるという効果が得られる。

る。

【図面の簡単な説明】

【図1】本発明の一実施例による情報販売システムの構成を示すブロック図である。

【図2】本発明の一実施例による情報販売システムの動作を示すフローチャートである。

【図3】図2のチケット要求処理を示すフローチャートである。

【図4】図2のチケット要求確認処理を示すフローチャートである。

【図5】本発明の一実施例における送信規約管理表の一例を示す図である。

【図6】本発明の一実施例における送信規約の一例を示す図である。

【図7】本発明の一実施例におけるアカウント管理表の一例を示す図である。

【図8】図1のチケットサーバ装置における決済センタへアカウント情報の正当性確認を委譲するための構成の一例を示す図である。

【図9】図2の課金処理を示すフローチャートである。

【図10】図1のチケットサーバ装置における決済センタを用いて課金処理を行うための構成の一例を示す図である。

【図11】図2のチケット生成処理を示すフローチャートである。

【図12】本発明の一実施例におけるチケットのフォーマットの一例を示す図である。

【図13】図2のチケット受信処理を示すフローチャートである。

【図14】図2の情報要求処理を示すフローチャートである。

【図15】図2の情報抽出処理を示すフローチャートである。

【図16】本発明の一実施例における情報管理表の一例を示す図である。

【図17】図2のパケット送出処理を示すフローチャートである。

【図18】図2の情報再生処理を示すフローチャートである。

【図19】本発明の一実施例による情報販売システムの具体例を示すブロック図である。

【図20】図19の情報販売システムにおける情報販売手続きを示すフローチャートである。

【図21】図19のチケットサーバ装置において課金履歴に基いて課金処理を行うための構成の一例を示すブロック図である。

【図22】本発明の他の実施例による情報販売システムの構成を示すブロック図である。

【図23】本発明の他の実施例による情報販売システムの動作を示すフローチャートである。

【図24】図23の第2のチケット要求確認処理を示すフローチャートである。

【図25】本発明の他の実施例における第2の情報識別子のフォーマットの一例を示す図である。

【図26】本発明の他の実施例における送信規約グループ管理表の一例を示す図である。

【図27】本発明の別の実施例による情報販売システムの構成を示すブロック図である。

【図28】本発明の別の実施例による情報販売システムの動作を示すフローチャートである。

【図29】図28の第2の情報抽出処理を示すフローチャートである。

【図30】図28のセッション鍵要求処理を示すフローチャートである。

【図31】図28のセッション鍵生成処理を示すフローチャートである。

【図32】図28のセッション鍵受信処理を示すフローチャートである。

【図33】図28の第2のパケット送出処理を示すフローチャートである。

【図34】図28の第2の情報再生処理を示すフローチャートである。

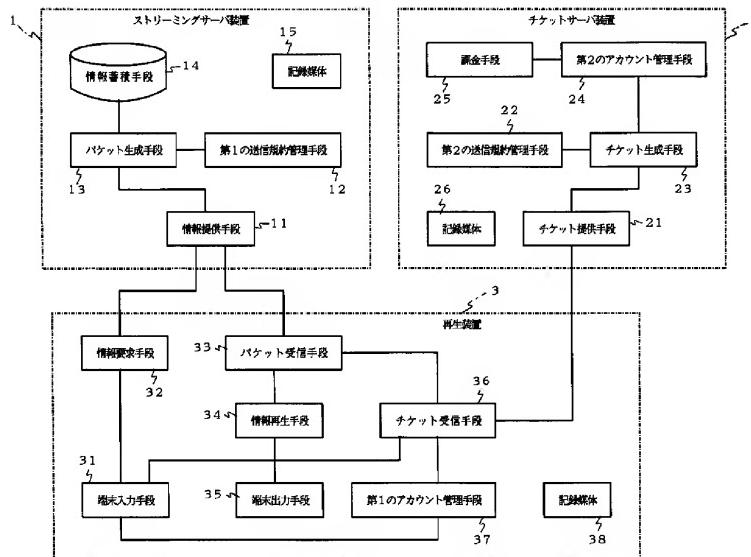
【符号の説明】

- 1 ストリーミングサーバ装置
- 2 チケットサーバ装置
- 3 再生装置
- 4 決済センタ
- 5 課金ログデータベース
- 6 第2のチケットサーバ装置
- 7 第2のストリーミングサーバ装置
- 8 第2の再生装置
- 1 1 情報提供手段
- 1 2 第1の送信規約管理手段
- 1 3 パケット生成手段
- 1 4 情報蓄積手段
- 2 1 チケット提供手段
- 2 2, 2 2-1~2 2-N 第2の送信規約管理手段
- 2 3 チケット生成手段
- 2 4 第2のアカウント管理手段
- 2 5 課金手段
- 3 1 端末入力手段
- 3 2 情報要求手段
- 3 3 パケット受信手段
- 3 4 情報再生手段
- 3 5 端末出力手段
- 3 6 チケット受信手段
- 3 7 第1のアカウント管理手段
- 6 1 第2の送信規約管理手段
- 7 1 第1のセッション鍵確立手段
- 7 2 第2のパケット生成手段

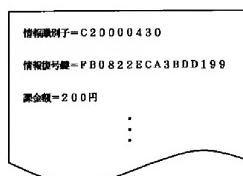
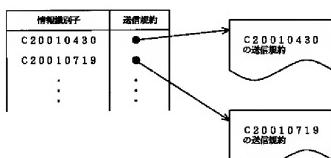
- 33
 8.1 第2のセッション鍵確立手段
 8.2 第2のパケット受信手段
 P.1 ストリーミングシステム運用者

- * P.2 情報の販売者
 P.3 ユーザ
 *

【図1】



【図5】



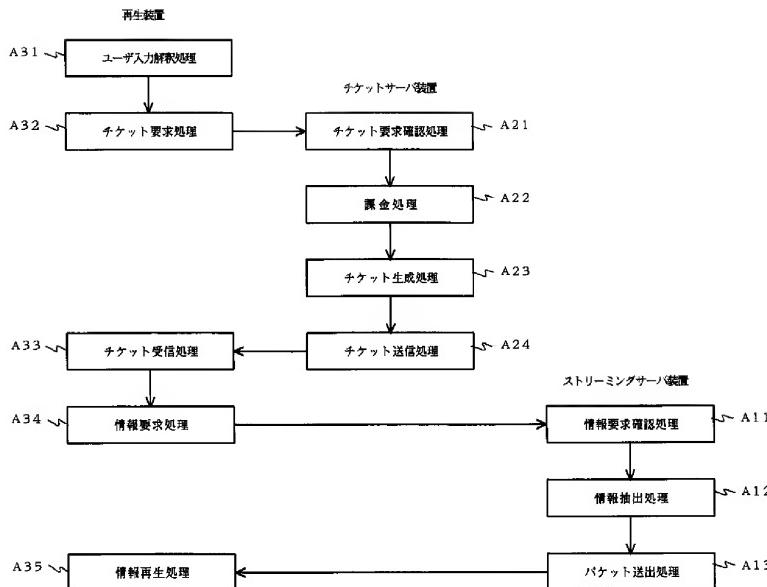
【図6】



【図25】



【図2】



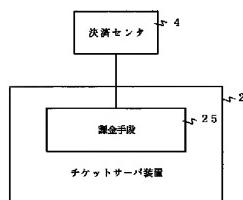
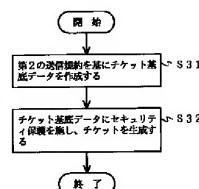
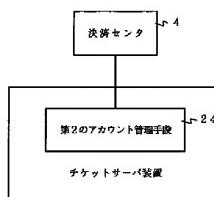
【図7】

【図8】

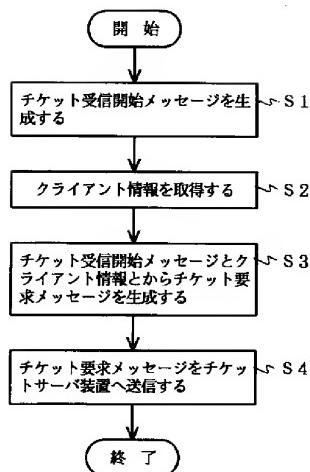
【図11】

情報識別子	パスワード	口座番号	...
...
U1002011	WB33BAX	09382653	...
U1002012	GM*2jfnb	18923557	...
...

【図10】



【図3】



【図12】

シリアル番号	TK2001080112345
情報識別子	C20010430
ユーザID	U1002011
情報復号鍵	FB0822ECA3BDD199
発行年月日	2001年08月01日
有効期限	2001年08月01日

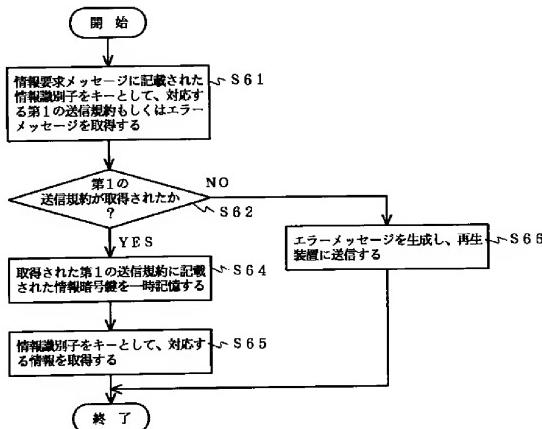
【図13】



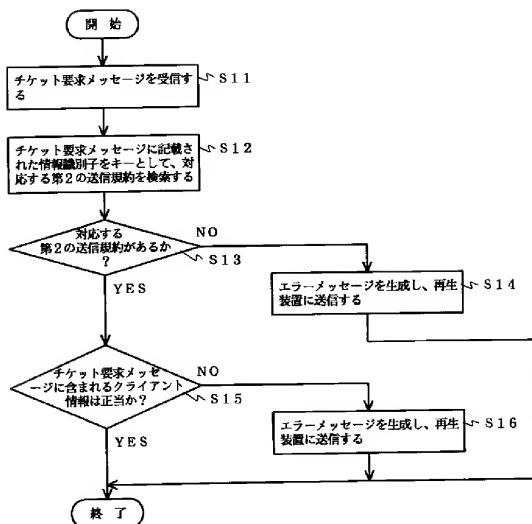
【図14】



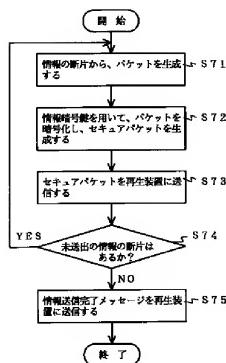
【図15】



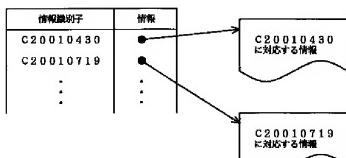
【図4】



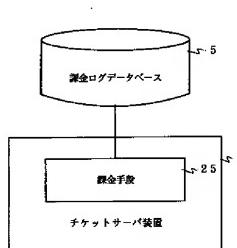
【図17】



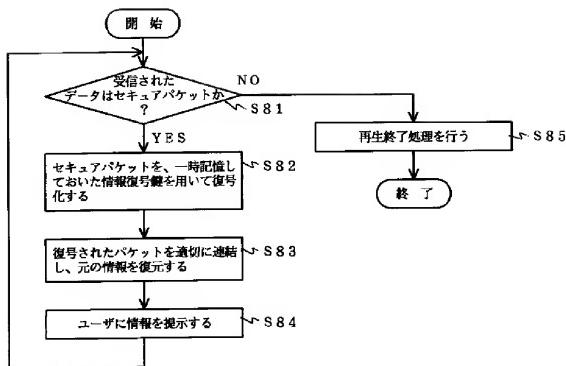
【図18】



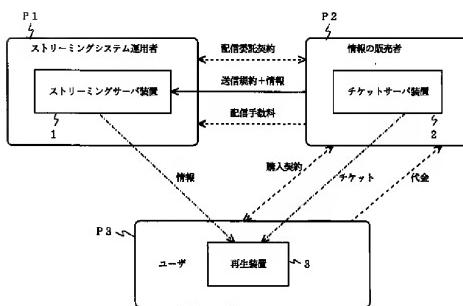
【図21】



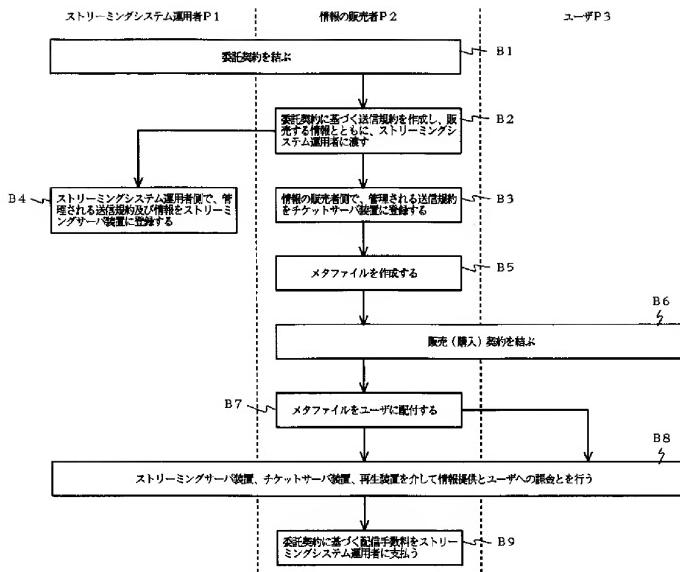
【図18】



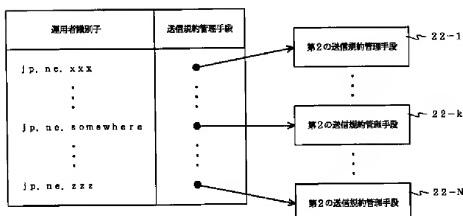
【図19】



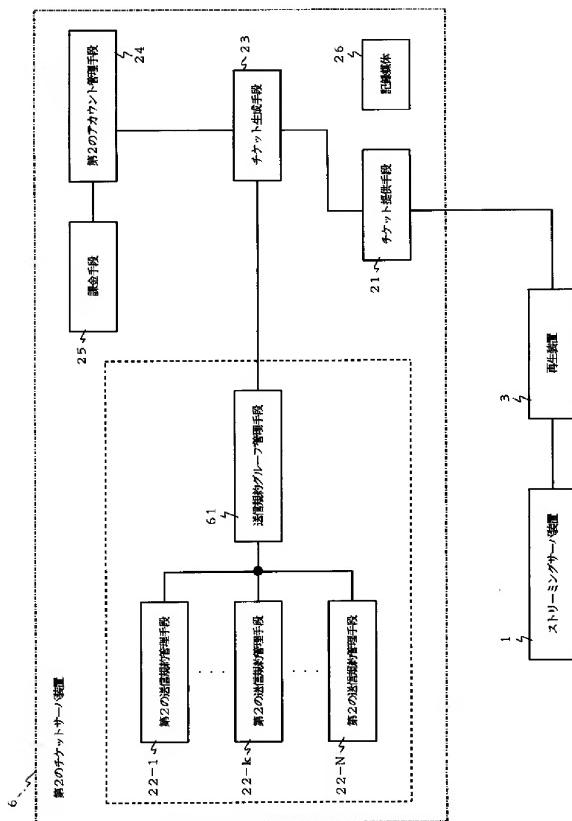
【図20】



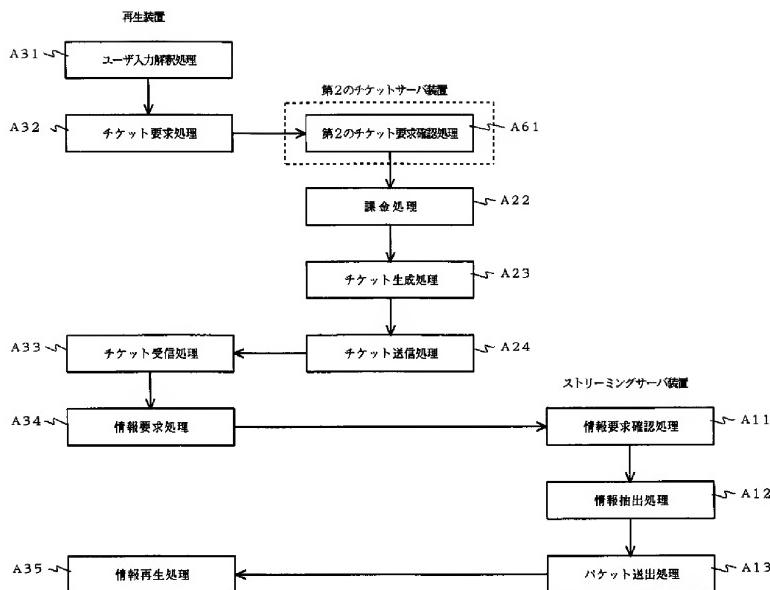
【図26】



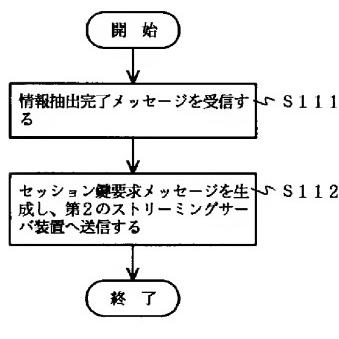
【図22】



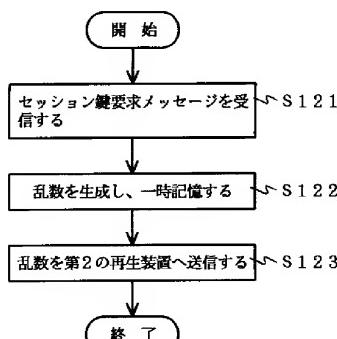
【図23】



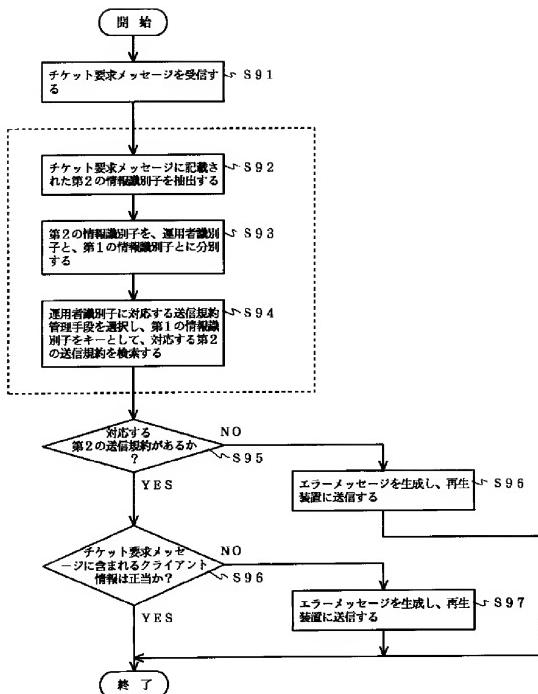
【図30】



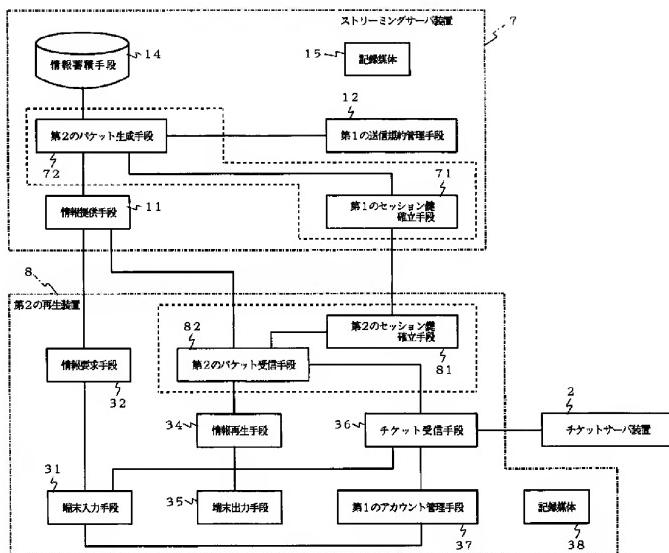
【図31】



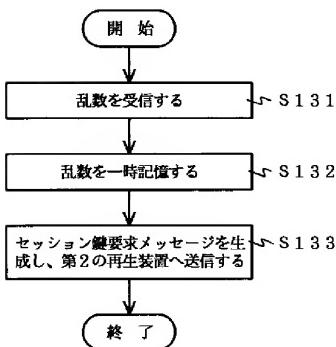
【図24】



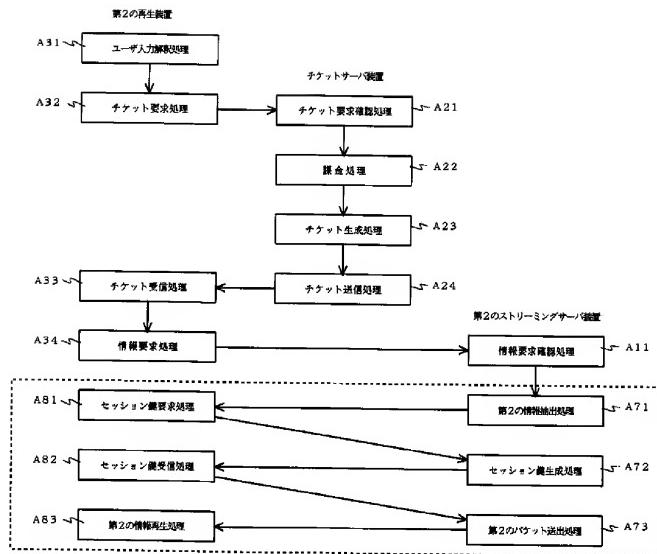
【図27】



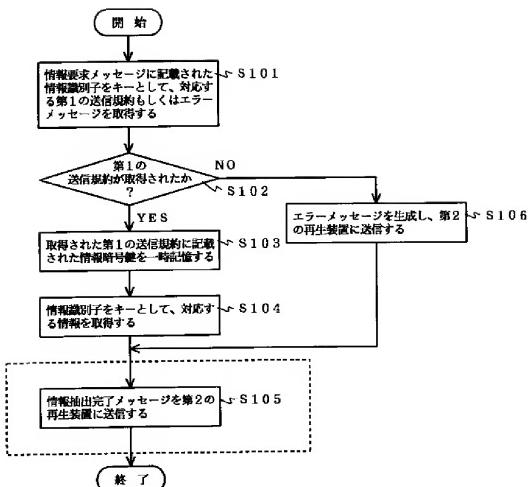
【図32】



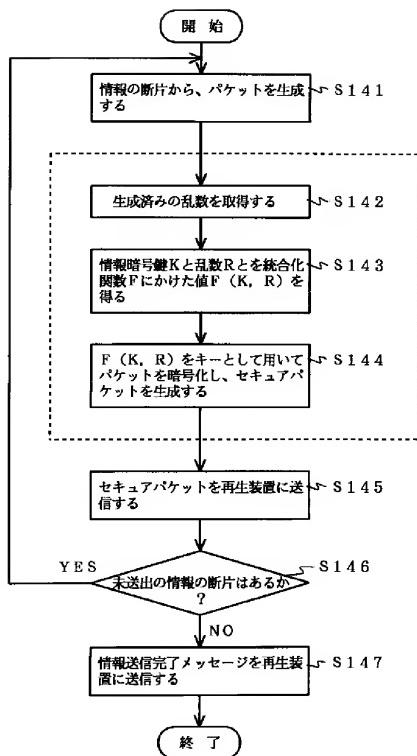
【図28】



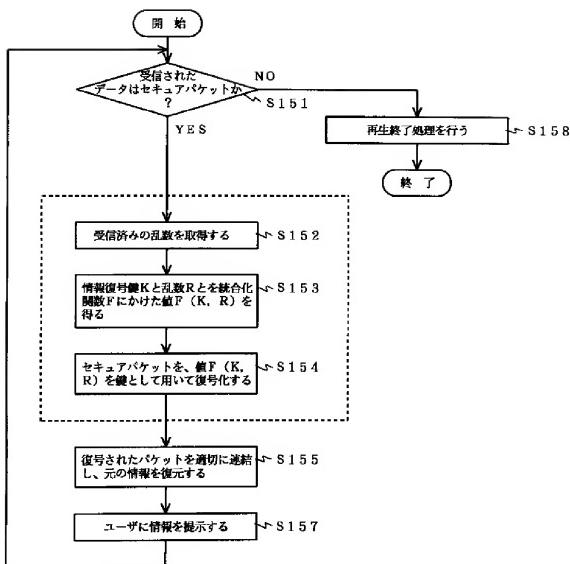
【図29】



【図33】



【図34】



フロントページの続き

(51)Int.CI.7	識別記号	F I	マークド (参考)
H 0 4 L	9/08	H 0 4 N	6 1 0 Z
	9/32		Z
H 0 4 N	7/167	H 0 4 L	6 0 1 B
	7/173		6 7 3 A
	6 1 0		

F ターム(参考) 5C064 BA07 BB01 BB02 BC04 BC06
BC17 BC18 BC22 BC23 BD02
BD08 BD09 CA14 CB01 CC01
CC04
5J104 AA01 AA07 AA16 EA01 EA04
KA01 NA02 PA07 PA11